RECEIVED
CENTRAL FAX CENTER

MAY 0 9 2006

Yee & Associates, P.C.

4100 Alpha Road
Suite 1100
Dallas, Texas 75244

Main No. (972) 385-8777
Facsimile (972) 385-7766

Facsimile Cover Sheet

To: Commissioner for Patents for **Examiner Longbit Chai** Group Art Unit 2131	Facsimile No.: **571/273-8300**
From: Candace Crawford Legal Assistant to Cathrine Kinslow	No. of Pages Including Cover Sheet: **25**

Message:

Enclosed herewith:

- Transmittal of Appeal Brief; and
- Appeal Brief.

Re: Application No. **09/931,301**
Attorney Docket No: **AUS920010242US1**

Date: Tuesday, May 9, 2006

Please contact us at (972) 385-8777 if you do not receive all pages indicated above or experience any difficulty in receiving this facsimile.

PLEASE CONFIRM RECEIPT OF THIS TRANSMISSION BY FAXING A CONFIRMATION TO 972-385-7766.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Black et al.**

Serial No.: **09/931,301**

Filed: **August 16, 2001**

For: **Presentation of Correlated Events as Situation Classes**

§ Group Art Unit: **2131**

§

§ Examiner: **Longbit Chai**

§

§ Attorney Docket No.: **AUS920010242US1**

§

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (571) 273-8300 on May 9, 2006.

By: Nancy Mikinkovich
Nancy Mikinkovich

35525
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

TRANSMITTAL OF APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:
ENCLOSED HEREWITH:

- Appeal Brief (37 C.F.R. 41.37)

No fees are believed to be required. If, however, any fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

Respectfully submitted,

Cathrine K. Kinslow
Registration No. 51,886

Duke W. Yee
Registration No. 34,285
YEE & ASSOCIATES, P.C.
P.O. Box 802333
Dallas, Texas 75380
(972) 385-8777
ATTORNEYS FOR APPLICANTS

RECEIVED
CENTRAL FAX CENTER
MAY 0 9 2006

Docket No. AUS920010242US1

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Black et al.**	§	Group Art Unit: **2131**
Serial No. **09/931,301**	§	Examiner: **Longbit Chai**
Filed: **August 16, 2001**	§	
For: **Presentation of Correlated Events as Situation Classes**	§	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

35525
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (571) 273-8300 on May 9, 2006.
By: Nancy Millikovich
Nancy Millikovich

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on April 24, 2006.

No fees are believed to be required. If, however, any fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-21

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: NONE
2. Claims withdrawn from consideration but not canceled: NONE
3. Claims pending: 1-21
4. Claims allowed: NONE
5. Claims rejected: 1-21
6. Claims objected to: NONE

C. CLAIMS ON APPEAL

The claims on appeal are: 1-21

STATUS OF AMENDMENTS

There are no amendments after final rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

A. CLAIMS 1, 8 and 15 - INDEPENDENT

Independent claims 1, 8, and 15 of the present invention are directed to a method, a computer program product, and a data processing system for reporting security situations, comprising the steps of logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute; classifying events as groups by aggregating events with at least one attribute within the event set as an identical value; calculating severity levels for the groups, wherein a severity level for a group is a function of a number of events comprising the group and values of common elements in the group; and reporting a group from the groups to a user as a situation, if a severity level of the group exceeds a threshold value. (Specification page 16, lines 15-28, Figure 9, and page 12, line 29 to page 13, line 7).

B. CLAIMS 2, 9 and 16 - DEPENDENT

Dependent claims 2, 9, and 16 of the present invention are directed to a method, a computer program product, and a data processing system wherein the severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups.. (Specification page 12, line 24 to page 13, line 32).

C. CLAIMS 4, 11 and 18 - DEPENDENT

Dependent claims 4, 11, and 18 of the present invention are directed to a method, a computer program product, and a data processing system which further comprise calculating the threshold value based on at least one of the source attribute of the event sets within the group, the target attribute of the event sets within the group, the event category attribute in each event set of the group, and the number of attributes in each event set of the group that are held constant across all of the event sets in the group. (Specification page 13, lines 8-32).

D. CLAIMS 7, 14 and 21 - DEPENDENT

Dependent claims 7, 14, and 21 of the present invention are directed to a method, a computer program product, and a data processing system which further comprise aggregating a subset of the groups into a combined group. (Specification page 14, lines 7-28).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. GROUND OF REJECTION 1 (Claims 1-21)

Claims 1-21 stand rejected under 35 U.S.C. § 103 as obvious in view of Farley et al. (U.S. Patent App. 2002/0078381) and Drake et al. (U.S. Patent No. 6,347,374).

B. GROUND OF REJECTION 2 (Claims 4, 7, 11, 14, 18, and 21)

Claims 4, 7, 11, 14, 18, and 21 stand rejected under 35 U.S.C. § 103 as obvious in view of Farley et al. (U.S. Patent App. 2002/0078381), Drake et al. (U.S. Patent No. 6,347,374), and Burrows et al. (U.S. Patent No. 2002/0073338).

ARGUMENT

A. GROUND OF REJECTION 1 (Claims 1-21)

A.1. 35 U.S.C. § 103, Obviousness, Claims 1-21

The Final Office Action rejects claims 1-21 under 35 U.S.C. § 102(e) as being obvious in view of Farley (U.S. Patent App. 2002/0078381) (hereinafter "*Farley*") and Drake (U.S. Patent No. 6,347,374) (hereinafter "*Drake*"). This rejection is respectfully traversed.

As to claims 1, 8, and 15, the Final Office Action states:

> As per claims 1, 8, and 15, Drake teaches a method in a data processing system for reporting security situations, comprising the steps of:
>
> logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute (Farley see example, Para [0019] Line 1-3 and Para [0019] Line 12 - 17: SRC / DEST / EVENT TYPE as the event attribute parameters);
>
> Farley teaches classifying and correlating the raw events (Farley, Para [0019] Line 1 - 3). However, Farley does not disclose expressly classifying events as groups by aggregating events with at least one attribute within the event set as an identical value.
>
> Drake teaches classifying events as groups by aggregating events with at least one attribute within the event set as an identical value (Drake, see example, Column 11 Line 38 - 50 and Column 14 Line 18 - 21: Drake teaches aggregating the correlated raw events into event groups with at least one attribute within the event set as an identical value such as (a) same user ID, or (b) same group type as "authentication failure" to generate an alert of severity situations).
>
> calculating severity levels for the groups, wherein, a severity level for a group is a function of a number of events comprising the group and values of common elements in the group (Drake, see example, Column 12 Line 29 - 30, Column 11 Line 38 - 50 and Column 14 Line 18 - 21: the "authentication failure" is qualified to meet the severity level as an event caused by the failures of a user login).
>
> reporting a group from the groups to a user as a situation, if a severity level of the group exceeds a threshold value (Drake, see example, Column 11 Line 38 - 50 and Column 14 Line 18 - 21: the "authentication failure" is qualified to meet the severity level as an event caused by the failures of a user login when the aggregating events exceed the predetermined number (i.e., threshold = 3) as taught by Drake).
>
> It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Drake within the system of Farley because (a) Farley teaches classifying and correlating raw events by providing a security management system in a networked computer system

(Farley, Para [0019] Line 1 - 3 and Para [0016]) and (b) Drake teaches improving network security by providing an effective event detecting systems (Drake, see example, Column 2 Line 4 - 8 and Column 3 Line 34 - 35).

Office Action dated January 24, 2006, pages 3-4.

The Examiner bears the burden of establishing a *prima facie* case of obviousness based on the prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). To establish a *prima facie* case of obviousness, the Examiner must show some suggestion or motivation to combine or modify reference teachings, show a reasonable expectation of success, and show that the cited references teach or suggest all of the claim limitations. MPEP § 706.02(j).

Independent claim 1, which is representative of independent claims 8 and 15 with regard to similarly recited subject matter, reads as follows:

> 1. A method in a data processing system for reporting security situations, comprising the steps of:
> logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute;
> classifying events as groups by aggregating events with at least one attribute within the event set as an identical value;
> calculating severity levels for the groups, wherein a severity level for a group is a function of a number of events comprising the group and values of common elements in the group; and
> reporting a group from the groups to a user as a situation, if a severity level of the group exceeds a threshold value.

The Examiner states that *Farley* does not teach classifying events as groups by aggregating events with at least one attribute within the event set as an identical value. As *Farley* does not teach or suggest classifying events a groups, *Farley* does not teach or suggest calculating severity levels for the groups, wherein a severity level for a group is a function of a number of events comprising the group and values of common elements in the group, nor does the Examiner allege that any section of *Farley* does so.

Drake does not cure the deficiencies of *Farley*. The Examiner alleges that *Drake* teaches calculating a severity level for the groups, wherein a severity level for a group is a function of a number of events comprising the group and values of common elements in the group, in the

following cited passages below:

> Information such as the event detection system event number and severity level are derived by this method.

Drake, col. 12, lines 29-30.

> In the present embodiment, there are six, standard, defined severity levels, one of which is assigned to each Virtual Record.

Level	Meaning
0	Irrelevant or undefined
1	Potentially significant event
2	Interesting event
3	Significant event
4	warning
5	Alert

Drake, col. 11, lines 38-50.

> For example, consider a set of rules that generates an alert on three failed logins. The rules for this alert are "three failed logins, by a user, at a platform, without an intervening successful login or system restart".

Drake, col. 14, lines 18-21.

The first passage above discloses that a rules-based processing method applied to an event record when the record is inserted into the database is used to derive an event detection system event number and severity level. The second passage discloses the various severity levels, such as irrelevant, potentially significant, interesting, significant, warning, and alert, and that each record is assigned one of the severity levels. The third passage discloses a rules-based alert which generates an alert based on three failed logins by a user.

However, the passages above do not teach or suggest calculating severity levels for the groups, wherein a severity level for a group is a function of a number of events comprising the group and values of common elements in the group. The passages merely disclose the use of assigning a severity level to a record, and that the rules-based alert may be used to generate an alert upon the failure of a user's 3rd login attempt. There is no discussion in *Drake* of calculating a severity level for a group of events as recited in the claimed invention. The Examiner alleges that "authentication failure" is qualified to meet the severity level as an event by the failures of a

user login. However, determining whether an alert should be generated based on multiple unsuccessful logins is not the same as calculating a severity level for a group of events. Rather, as shown above in column 11, lines 38-50 and column 12, lines 28-30, *Drake* does not teach assigning severity levels to groups of events, but rather *Drake* explicitly teaches that one severity level is assigned to each Virtual Record. As disclosed in column 6, lines 6-8, *Drake* teaches that a Virtual Record is a "standardized flat representation of an event in a normalized format". Thus, even though *Drake* derives security levels, these levels are derived for each Virtual Record, which represent a single event, rather than a group of events as recited in claim 1. *Drake* does not mention that there is a severity level calculated for the group itself. Instead, *Drake* discloses an alert is generated if a specific number of the same event occurs (e.g., 3 failed logins by a particular user).

Furthermore, the passages above also do not teach or suggest that the severity level for a group is a function of a number of events comprising the group and values of common elements in the group. Thus, the common elements in the group have values which are used to calculate the severity level of the group. *Drake* does not mention a severity level calculated for the group itself and that the severity level of the calculated group is based on common elements in the group. *Drake* merely discloses that an alert is generated based on the occurrence of a specific number events (e.g., 3 failed logins).

Thus, while *Drake* may use a derive and assign severity levels to individual records in the database tables, *Drake* does not teach or suggest anything about calculating a severity level for a group of events, nor does *Drake* teach or suggest that the calculated group severity level is based on a number of events comprising the group and values of common elements in the group. Even if the missing elements of the rejected claims existed in the prior art, for the rejected claims to be obvious there must be some motivation or incentive from the prior art to modify or combine the reference teachings to achieve the present invention. The Examiner does not provide any motivation from either reference that making all the necessary modifications to the reference teachings to achieve the present invention would be desirable. If the Examiner cannot make such a showing, then the Examiner has simply relied on hindsight with the benefit of Applicants' disclosure to develop an incentive for the changes, which in fact, would not be obvious to one of ordinary skill in the art at the time the invention was made.

In view of the above, Applicants submit that independent claims 1, 8, and 15 are not taught or suggested by the alleged combination of *Farley* and *Drake*. At least by virtue of their dependency on claims 1, 8, and 15, respectively, *Farley* and *Drake* also do not teach or suggest the features in dependent claims 2-7, 9-14, and 16-21.

Furthermore, claims 2-7, 9-14, and 16-21 recite additional subject matter not suggested by the *Farley* and *Drake* references. For instance, claims 2, 9, and 16 recite severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups. As discussed in the response to the rejection of claims 1, 8, and 15 above, the features of calculating severity levels for an event group in these claims are neither taught nor suggested by *Farley* or *Drake*.

Accordingly, Applicants respectfully request withdrawal of the rejection of claims 1-21 under 35 U.S.C. §103.

B. GROUND OF REJECTION 2 (Claims 4, 7, 11, 14, 18, and 21)

B.1. 35 U.S.C. § 103, Obviousness, Claims 4, 7, 11, 14, 18, and 21

The Final Office Action rejects claims 4, 7, 11, 14, 18, and 21 under 35 U.S.C. § 103 as being obvious in view of Farley (U.S. Patent App. 2002/0078381) (hereinafter "*Farley*"), Drake (U.S. Patent No. 6,347,374) (hereinafter "*Drake*"), and Burrows et al. (U.S. Patent No. 2002/0073338) (hereinafter "*Burrows*"). (While the Examiner specifies in the Final Office Action that *Farley* teaches the features in dependent claims 4, 7, 11, 14, 18, and 21, the Examiner does not actually cite to or point out any section of *Farley* as teaching these claims. Instead, the Examiner cites to *Burrows* as teaching the limitations in claims 4, 7, 11, 14, 18, and 21.) This rejection is respectfully traversed.

Claims 4, 7, 11, 14, 18, and 21 are dependent claims depending from claim 1, 8, and 15, respectively. Claims 4, 7, 11, 14, 18, and 21 are patentable over the cited references because the combination of the *Burrows* reference with *Farley* and *Drake* would not reach the presently claimed invention. The features relied upon as being taught in the *Farley* and *Drake* references

are not taught or suggested by those references, as argued in the response to the rejection of claims 1, 8, and 15 in section A.1 above. As a result, a combination of these references would not reach the claimed invention in claims 4, 7, 11, 14, 18, and 21.

Furthermore, claims 4, 7, 11, 14, 18, and 21 recite additional subject matter not suggested by the *Farley*, *Drake*, or *Burrows* references. For instance, claims 7, 14, and 21 recite aggregating a subset of the event groups into a combined group. The Examiner points to the following passages in *Farley* and *Burrows* as teaching this feature:

> Referring now to Figure 5D, this Figure is a functional block diagram illustrating an exemplary Attack From Attacked Host (AFAH) computer security threat. Figure 5D illustrates a computer incident source 503 with an Internet protocol address of 1.1.1.1 sending an attack to host (attacked host) 505 that has an Internet protocol address of 2.2.2.2. The attack between the computer incident source 503 and the attacked host 505 may be characterized as a raw computer event I. After being attacked, the attacked host 505 then sends another attack to a second host 507, having an Internet protocol address of 3.3.3.3. The attack between the attacked host 505 and the second host 507 may be characterized as a second raw event II. The second host 507 generates an attack on a third host 509, having an Internet protocol address of 4.4.4.4. The attack between the second host 507 and third host 509 may be characterized as a third raw event III.

Farley, para [0079].

> In one embodiment, the packet traffic monitor observes the network and thereby detects and localizes all broadcast packets traffic. Observing more than a predetermined number of broadcast packets within a predetermined time period implies that a broadcast storm is underway. It is likely that the packet is correctly addressed, and that knowing the source MAC address and the network topology will point to a particular port of a forwarding device, e.g., switch port, to be disabled. In another embodiment, the per-port broadcast ingress packet counters can be used to trace broadcast packets to their source. This approach is used if the packet traffic monitor fails at determining the source, possibly because of incorrectly formatted packets or because the misbehaving host has not been seen on the network before (unknown MAC address). This detection approach is less timely than the prior approach since the process of retrieving these counters from the switch is extensive and it cannot be executed often.

Burrows, para [0050].

> For example, the monitor can detect too many packets destined to an overloaded server, too many probe packets directed to a firewall or too many ARP request packets.

Burrows, para [0046] line 10-11.

As can be seen from the cited paragraphs above, neither *Farley* nor *Burrows* mentions aggregating a subset of an event group into a combined event group, as recited in claims 7, 14, and 21.

Accordingly, Appellants respectfully request the withdrawal of rejection of claims 4, 7, 11, 14, 18, and 21 under 35 U.S.C. § 103.

Cathrine K. Kinslow
Reg. No. 51,886
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

CLAIMS APPENDIX

The text of the claims involved in the appeal are:

1. A method in a data processing system for reporting security situations, comprising the steps of:

logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute;

classifying events as groups by aggregating events with at least one attribute within the event set as an identical value;

calculating severity levels for the groups, wherein a severity level for a group is a function of a number of events comprising the group and values of common elements in the group; and

reporting a group from the groups to a user as a situation, if a severity level of the group exceeds a threshold value.

2. The method of claim 1, wherein the severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups.

3. The method of claim 1, wherein the events include at least one of a web server event, an electronic mail event, a Trojan horse, denial of service, a virus, a network event, an authentication failure, and an access violation.

4. The method of claim 1, further comprising:

calculating the threshold value based on at least one of the source attribute of the event sets within the group, the target attribute of the event sets within the group, the event category attribute in each event set of the group, and the number of attributes in each event set of the group that are held constant across all of the event sets in the group.

5. The method of claim 1, wherein the target attribute represents one of a computer and a collection of computers.

6. The method of claim 1, wherein the source attribute represents one of a computer and a collection of computers.

7. The method of claim 1, further comprising:

aggregating a subset of the groups into a combined group.

8. A computer program product in a computer readable medium for reporting security events, comprising instructions for:

logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute;

classifying events as groups by aggregating events with at least one attribute within the event set as an identical value;

calculating severity levels for the groups, wherein a severity level for a group is a

function of a number of events comprising the group and values of common elements in the group; and

reporting a group from the groups to a user as a situation, if a severity level of the group exceeds a threshold value.

9. The computer program product of claim 8, wherein the severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups.

10. The computer program product of claim 8, wherein the events include at least one of a web server event, an electronic mail event, a Trojan horse, denial of service, a virus, a network event, an authentication failure, and an access violation.

11. The computer program product of claim 8, comprising additional instructions for:

calculating the threshold value based on at least one of the source attribute of the event sets within the group, the target attribute of the event sets within the group, the event category attribute in each event set of the group, and the number of attributes in each event set of the group that are held constant across all of the event sets in the group.

12. The computer program product of claim 8, wherein the target attribute represents one of a computer and a collection of computers.

13. The computer program product of claim 8, wherein the source attribute represents one of a computer and a collection of computers.

14. The computer program product of claim 8, comprising additional instructions for:

aggregating a subset of the groups into a combined group.

15. A data processing system for reporting security events, comprising:

a bus system;

a memory;

a processing unit, wherein the processing unit includes at least one processor; and

a set of instructions within the memory, wherein the processing unit executes the set of instructions to perform the acts of:

logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute;

classifying events as groups by aggregating events with at least one attribute within the event set as an identical value;

calculating severity levels for the groups, wherein a severity level for a group is a function of a number of events comprising the group and values of common elements in the group; and

reporting a group from the groups to a user as a situation, if a severity level of the group exceeds a threshold value.

16. The data processing system of claim 15, wherein the severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups.

17. The data processing system of claim 15, wherein the events include at least one of a web server event, an electronic mail event, a Trojan horse, denial of service, a virus, a network event, an authentication failure, and an access violation.

18. The data processing system of claim 15, wherein the processing unit executes the set of instructions to perform the act of:

calculating the threshold value based on at least one of the source attribute of the event sets within the group, the target attribute of the event sets within the group, the event category attribute in each event set of the group, and the number of attributes in each event set of the group that are held constant across all of the event sets in the group.

19. The data processing system of claim 15, wherein the target attribute represents one of a computer and a collection of computers.

20. The data processing system of claim 15, wherein the source attribute represents one of a computer and a collection of computers.

21. The data processing system of claim 15, wherein the processing unit executes the set of instructions to perform the act of:

aggregating a subset of the groups into a combined group.

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.